EXHIBIT D

UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA
(Alexandria Division)

QUETEL CORPORATION, Plaintiff, v. HISHAM ABBAS, et al., Defendants.	Case No. 1:17-CV-00471 (AJT-JFA)

DECLARATION OF MONTY G. MYERS

I, Monty G. Myers, declare as follows:

1. I hereby submit this declaration in support of Plaintiff Quetel Corporation's ("Quetel") Motion for Sanctions.

2. My name is Monty G. Myers. My date of birth is September 11, 1963 and my address is 3305 Northland Drive, Suite 305, Austin, Texas 78731.

3. I am Founder and CEO of Eureka Software Solutions, Inc. ("Eureka Software"), a custom software development and IT services company based in Austin, Texas.

4. I have over thirty (30) years of experience in the software industry with a substantial portion of my work over this period involving the conceiving, planning, architecting, designing, developing, testing, launching, and maintaining commercial software solutions/products.

5. I have a Bachelor of Science degree in Engineering from Texas A&M University, *cum laude*, and completed substantial graduate level course work at the University of Texas. I am a licensed Professional Engineer in the State of Texas, and I hold patents in the area of load performance testing for distributed Internet software applications/systems.

6. I am involved in most aspects of daily management, operational, and technical tasks at Eureka Software, including business development, contracts, customer relations, project planning, execution, and oversight. I have negotiated and performed hundreds of software and technology contracts and statements of work involving complex software projects and licensing terms and have been actively engaged in protecting confidential technology of Eureka Software and its clients. I have performed in this capacity at Eureka Software for over 30 years.

7. During my time at Eureka Software, the company and I personally have worked on, had access to, and been responsible for creating and working with the most sensitive and often complex software, source code, and other materials for hundreds of clients, including recognizable names such as Apple, Samsung, American Airlines, AT&T, AMD, IBM, Chevron, Motorola, Progressive Insurance, Siemens, UBS, Xerox, and many more.

8. In addition to my industry experience, I have served as an expert consultant/witness in over eighty (80) complex litigation matters over the years in both state and federal court. I have testified extensively at trials, hearings, and in depositions for these cases. Most of these engagements have involved disputes concerning technology services performance under contract and/or software and technology-related trade secrets and patents, many of which required expert review and analysis of one or both party's software, source code, and other similar materials. The parties in these cases have ranged from sophisticated startups, to the largest, well-known multinational, public companies, to sovereign governments and government agencies.

9. I am experienced in the review and comparison of software source code and functionality in relation to contractual commitments and requirements and/or protected intellectual property including, but not limited to, trade secrets, copyrights and patents. I am also experienced

in the field of digital forensics, which includes forensic examination of the contents of electronic devices.

10. I have been engaged as an expert for Quetel in the above-captioned case with respect to certain issues pertaining to the comparison of Quetel's Traq Suite 6 software, including its source code and related elements, with Defendant finalcover, LLC's ("finalcover") software known as CaseGuard, including its source code and related elements.

11. I have reviewed the Complaint, Defendants' Answer, Quetel's First Set of Interrogatories and Requests for Production of Documents to Defendant finalcover, LLC, Quetel's First Set of Interrogatories and Requests for Production of Documents to Defendant Hisham Abbas, Quetel's First Set of Interrogatories and Requests for Production of Documents to Defendant Shorouk Mansour, the Transcript of the July 21, 2017 Hearing on Quetel's Motion to Compel and for Extension of Expert Disclosure Deadline, certain other documents produced by the parties in discovery in this matter prior to the date of this declaration, a letter from Counsel for Quetel to Defense Counsel, dated August 25, 2017 ("Quetel August 25, 2017 Letter"), and a letter from Defense Counsel to Counsel for Quetel, dated August 31, 2017 ("Defense August 31, 2017 Letter"). I have also reviewed software source code provided to me by Quetel and Defendants. More specifically, I was provided with the following versions of source code for TraQ Suite 6 and for CaseGuard: 1) a 2014 version of TraQ6 source code and 2) a version of CaseGuard source code showing last modified file dates in mid-2017 (May through July 2017)[1]. I note here that I have been provided two versions of CaseGuard's source code, despite Defendants' statements that only one version has ever existed.

[1] Another version of the CaseGuard source code was provided via a logical image of the 'Development' folder but my analysis indicated that it was it was substantially similar to the CaseGuard source code described above, although it was a distinct, second version.

12. In addition, I have reviewed and forensically analyzed forensic images of two hard drives, identified as LID_167845 and LID_167846 which were produced by Defendants in this matter. These images were taken from the same computer which Defendants have claimed is the only computer used in the development of CaseGuard that is still in their possession, custody or control.

13. A significant element of our expert analysis was a direct comparative analysis of the versions of the QueTel's TraQ Suite 6 software/source code and the Defendants' CaseGuard software/source code that I was provided. The goal of this analysis was to determine whether or not there was evidence that QueTel's source code may have been directly or indirectly used by Defendants in their development of a competing product.

14. The results of my comparative analysis clearly indicate both access to and use of QueTel's TraQ Suite 6 source code within Defendants' CaseGuard software as described in my full expert report.

15. As a result of my review of the TraQ Suite 6 and CaseGuard code, I found that there are instances of fairly direct usage of the TraQ Suite 6 code in the CaseGuard code, as well as more indirect usage, where the original TraQ Suite 6 source code and structure was refactored somewhat but still reflective of the original source code. Many of the differences between TraQ Suite 6 and CaseGuard involve changes in class names, variable names and property names that could be easily done through a "Find and Replace" command in a code editing software package, with such change not impacting the functionality or performance of the software. Other differences involve changes in the code syntax while the overall logic of the software was kept substantially the same. The lack of identical source code texts, in my opinion, appears to be the result of substantial refactoring, if not obfuscation, on the part of Defendants. Many of the changes had no

material functional relevance, but seem to have been made for the sole purpose of changing the visual expression of the code. In fact, in my many years of experience in the industry and in providing expert services for copyright and trade secret matters, this case represents some of the most substantial refactoring/obfuscation I have observed.

16. Some notable conclusions are listed below:

a. The structure of the CaseGuard software shares many common traits with the TraQ Suite 6 software. Not only are similar software classes used for similar purposes, but the names of the classes are often very close as well. Within the classes, property names, function names, and the logical structure of the classes in many cases are astonishingly close to one another. Even when considering individual functions, the parameter names, parameter types, variable names, and variable types share obvious similarities. While there are syntax differences between the TraQ Suite 6 code and CaseGuard code, the logic used within the code is often very close and in some cases almost the same. I have found this pattern repeatedly while comparing the two code bases. The layout and logic of the equivalent CaseGuard file is strikingly similar to TraQ except for name changes;

b. For example, many of the classes, functions, properties, and variables have names that seem to follow a formula for renaming. Many of these names in the TraQ Suite 6 software have the same names in the CaseGuard software, but have the prefix "CG" or "Guard" added to the names as a prefix. In other examples, the prefix "TraQ" has been replaced with the prefix "CG" or "Guard" for class names, property names, function names, and variable names throughout the CaseGuard code.

c. In general, it is clear to me that there has been a global replace of certain keywords in the CaseGuard software projects. In my opinion, these naming similarities cannot be attributed

to mere coincidence, and it is clear to me that the CaseGuard code has been modified based on its origins as the TraQ Suite 6 software package.

17. I further analyzed the nature of these similarities to determine if there are potentially other explanations for the unmistakable similarities in the code. An inspection of the code as well as searches for this code from public sources did not indicate any alternative source. Indeed, it is rather clear to persons skilled in the art that these similarities relate to areas where the programmer had creative choice and were not merely the product of the programmer basing his or her work on other public sources.

18. Based upon the above-described direct comparative analysis of the TraQ Suite 6 and CaseGuard source code, it is my finding that TraQ Suite 6 and CaseGuard share multiple similarities suggesting and an unmistakable common source code lineage. The nature of these similarities indicates that this is not a coincidence.

19. However, what my analysis could not accomplish, based on the materials that have been produced by the Defendants, is a direct, line-by-line comparison of the TraQ Suite 6 source code to prior versions of CaseGuard's source code, particularly the original or earliest versions of the CaseGuard code – the versions of the source code that would be most likely to contain evidence of literal copying of the TraQ Suite 6 source code. In my experience, these prior versions, and changes to them, are normally present and maintained by software developers on what is known in the software development industry as a source code control system.

20. The source code control system is one of the most important and informative artifacts for cases such as this involving expert analysis related to allegations of theft and copying of software source code. A source code control system is a standard industry tool used to manage the entire life cycle of the source code created by software engineers. It is the official repository

of record to contemporaneously capture all changes to the source code over time. These systems contain a detailed record of when software was created or added to a project as well as who made such changes and when they did so. There are several types source code control systems on the market, including Git, Subversion Source Code Control by Apache and Microsoft's Team Foundation Server.

21. Such systems allow software engineers to look at the software at any relevant date in the history of its development. This ability to roll back in time to a previous version of the software is vital to a software developer when, inevitably, problems arise with a new release of the software or a version thereof. The source code control system also serves as a backup, and preserves the software's source code to prevent against deletion, corruption or other loss of the source code. This same capability is also useful in the context of this matter in studying the evolution of a potentially misappropriated system over time. For example, it is useful to determine if a software application developed organically or whether it was based upon another software system.

22. It is standard practice within the software development industry to use a source code control system. Indeed, it is essentially unheard of for commercial software to be managed without the use of a source code control system. In my experience, this is true for both small software development firms and the largest worldwide enterprises, irrespective of the number of developers. Source code is the most important work product that software engineers create every day. Thus, it is important to maintain this complete history and to be able to revert and review historical versions when necessary. Importantly, source code control systems also contain various trial and/or research and development versions of the software that may not immediately make it to the current production software. It also contains removed or deprecated code. Finally, source

code control systems are used for version and client/custom traceability management; when different users have different versions of the software, the source code control system helps ensure the development team is reviewing the appropriate version/product for each client or situation. Again, it is unthinkable that any reasonable developer would operate without using a source code control system.

23. In my experience as an expert in over eighty (80) matters, related to intellectual property, no single material has proven more important than source code control in clearly communicating critical elements of a product's development and the related project history behind the product. For purposes of a software source code comparison, like the one I have undertaken in this case, the source code control system used to develop the allegedly infringing code is often the single most critical piece of evidence. With access to the source code control system of the allegedly infringing code, the expert conducting the analysis of the code will generally be able to review the earlier versions of the allegedly infringing code and compare them with the applicable version of the code on which they allegedly infringe. Access to the earlier versions of the source code stored in a source code control system is particularly important where, as is the case here, there is significant evidence of refactoring/obfuscation of the source code text of the allegedly infringing code.

24. Defendants surprisingly initially claimed that they did not use such a system in developing CaseGuard. *See* Defendant finalcover's and Defendant Abbas's Answers to Interrogatory No. 5; Defendants' Answers to Document Request No. 44. This was highly unusual and is very unlikely in current software development practice, particularly for this type of software development project related to a commercial product.

25. It is also inconsistent with evidence I have reviewed in preparing my expert report in this matter. First, I received and reviewed a screen shot of the source code for CaseGuard (attached to the Complaint as Exhibit C). This screen shot shows Git bash client for Windows on the lower-left part of the screen. It also shows padlocks on the right. These padlocks indicate that version control is being used within the CaseGuard project that is being developed using Microsoft Visual Studio. This, by itself, shows that Defendants were using a source code control system at the time of the social media discussion represented in the screenshot, which I understand to be on or about July 30, 2014. A copy of the screenshot, highlighting these points is attached hereto as Exhibit 1.

26. After producing forensic images of hard drives for a device used for CaseGuard development, Defendants, and in particular Mr. Abbas, have since restated their position in letter dated August 31, 2017, to counsel for QueTel. In that letter, Mr. Abbas represents the following: "(1) while a source code control system was installed on his 'old computer,' he did not use it to develop CaseGuard; (2) he copied his old computer's contents to a new computer but did not install a source code control system on his new computer; (3) the forensic copy of his new computer did not contain a source code control system because he did not install one; and (4) he does not have access to his old computer because it was disposed of in late 2016." August 31, 2017 letter from Albert Wilson to Timothy J. McEvoy and Patrick J. McDonald, attached hereto as Exhibit 2.

27. I have reviewed the forensic images provided by Defendants pursuant to the Court's July 21, 2017 Order, and those images flatly contradict Mr. Abbas' statements concerning the CaseGuard code, as relayed in the August 31, 2017 letter.

28. As an initial matter, the forensic images produced by Defendants were not consistent with our understanding or expectations with respect to the production that Defendants

were ordered to make. Given that there is evidence of CaseGuard code being written as far back as 2014, we expected to be provided with images of the computers that were being used to develop CaseGuard in the 2014 timeframe.

29. From the computer that the Defendants made available, two images were created. Analysis of the images indicates that computer's drives were not the same ones that were being used during development of CaseGuard in 2014. Forensic analysis shows that the file systems for the Operating System/Applications partition and one of the data drive's partition were created in 2016, several months after a Cease and Desist letter was sent to the Defendants expressly informing them of their obligation to preserve evidence relevant to QueTel's claims in this matter.[2] Additionally, even though the other data partition shows a file system creation date of 2010, the creation dates of the user files on that partition match the same 2016 creation dates found on the other two partitions.

30. My forensic analysis also found clear evidence that one or more source code control systems were utilized by Defendant in conjunction with the CaseGuard product line. Forensic images show the use of the Subversion Source Code Control system with the CaseGuard Project. More specifically, my analysis revealed the existence of a folder - the ".svn folder" (shown in Exhibit 4 hereto) – which contains a revision of the CaseGuard software that was checked out from a server running the Subversion Version Control software – a source code control system. The files in this directory help the Subversion Version Control application recognize which source code files have been altered by the developer. The .svn Subversion folder was found in both forensic images that I received and analyzed. The dates of the files within this folder show a last written timestamp of January 5, 2015. Of note, we discovered this .svn folder only after performing a

[2] A true and accurate copy of that Cease and Desist Letter is attached hereto as Exhibit 3.

forensic analysis of the disk images created from the Defendant Abbas' computers. Remarkably, the materials previously produced in the case did not include these folders. Neither the zip file "Hisham Abbas - Lawyers Eyes Only.zip" contained on CD "CF-000001" nor the logical image of the \Development\CaseGuard folder "Finalcover_Development_CaseGuard_Folder.L01" contained these Subversion Version Control software related folders even though all evidence of source code control used for the CaseGuard project was requested to be produced. The fact that this source code control system had been clearly utilized for CaseGuard in the past was completely masked by Defendants' failure to reveal its existence. It was only through our detailed forensic review of the images that Defendants' produced in response to this Court's July 21, 2017 Order that we were able to discover the above referenced evidence of Defendants' use of the Subversion Version Control software.

31. To date, Defendants have not produced the source code control system that they used in developing the CaseGuard code.

32. I am not aware of any reasonable explanation as to why Defendants would not provide such critical information in response to the discovery requests issued in this case – particularly given that the information clearly existed on the Defendant Abbas' computers and is obviously relevant to the issues in this case. Defendant Abbas is an experienced software engineer and he would have known about and understood the importance of these files related to the source code control system.

33. Additionally, the forensic images show that Defendant Abbas used the Microsoft Visual Studio development environment. Visual Studio is an integrated development environment tool that is used by developers to create computer programs. It is the tool Defendant Abbas used for the development of the CaseGuard application. Visual Studio can be integrated with a source

code control system. The Facebook screenshot from 2014 likewise shows Abbas's use of Visual Studio for his development of CaseGuard and such screenshot further shows the use of source code controls at that time as described above. Indeed, my independent testing confirmed that the only way that the Visual Studio pane displays the series of source code control related icons is when Visual Studio is being utilized with a source code control system.

34. A matter that is equally concerning is that the forensic analysis showed an intentional deletion of the version control software "Git for Windows" right before defendant was to produce his computer for forensic imaging. Git is a free and widely-used Version Control System. Analysis of Abbas' user registry file showed that the Git for Windows application was installed and had a shortcut place on the taskbar of the admin user (Defendant Abbas) on September 26, 2016, the date many other applications were installed and files copied to the computer. That application was then uninstalled on July 20, 2017, just six days before the forensic company arrived to take images of the Defendant's device. (See Exhibit 5)

35. My forensic analysis of the produced images identified the following additional information to support the fact that Defendants had intentionally manipulated evidence for the purpose of the litigation:

a. The Operating System for the produced computer was installed on July 13, 2016, months after the Cease and Desist/Evidence Preservation letter was sent on May 16, 2016;

b. Applications for the produced computer (e.g., Microsoft Visual Studio, SQL server etc.) were all installed on or after September 26, 2016;

c. All user created folders on the development partition (including the 'Development' folder) were created on or after September 26, 2016;

d. The 'backups' folder on the backup partition which contains multiple backup versions of CaseGuard was created on September 26, 2016;

e. Evidence of a mass copy of CaseGuard code related files into the 'Development' folder shortly after the 'Development' folder was created on the partition on September 26, 2016;

f. Thousands of CaseGuard related files were deleted from the Backups data partition on July 7, 2017.

36. In sum, it is my opinion that, to a reasonable degree of professional certainty, Abbas is either suppressing or has destroyed his historical backups/copies (either in a source code control system or elsewhere), or he operated without any protection to secure his large body of development work. Based on my experience, and my above-stated analysis-based opinion that Defendants used source code control with CaseGuard, it is further my opinion that it is far more likely that Defendant Abbas suppressed or destroyed the historical source code and source code control system than it is that he did not use reasonable backup protection such as source code control. Indeed, the forensic evidence precludes a finding that Defendants never used a source code control system with CaseGuard.

37. In light of my observations of significant refactoring/obfuscation, the number and nature of the material similarities between the two software systems, and Defendants apparent suppression or destruction of historical source code and source code control system, it is my opinion that the most likely reasonable explanation of such observations is that the TraQ Suite 6 source code was originally copied by Defendants who then modified such source code over time.

38. Finally, it is my opinion, that if I had been provided access to the source code control system for the CaseGuard product, such system would have documented the detailed

historical changes to and evolution of the CaseGuard software – including the details of when and how Plaintiff's TraQ Suite 6 source code came to be introduced into Defendants' CaseGuard source code.

39. My conclusions have been presented to Defendants in the form of a report, which was produced to Defendants on September 5, 2017 as part of Plaintiff's Expert Disclosures. I have since been provided with a letter from Defendants' counsel dated September 14, 2017, responding to a letter from Plaintiff's counsel regarding my findings. Defense Counsel's letter (attached hereto as Exhibit 6), does not alter my analysis or conclusions as stated in this Declaration.

40. To the contrary, the September 14, 2017 letter contains important admissions that actually further support my opinions:

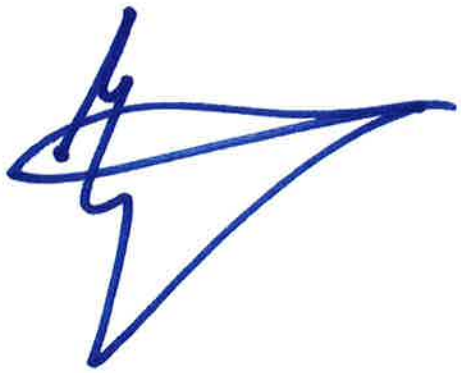
a. Defendant Abbas now admits that the Subversion source code control system was indeed used for at least parts of CaseGuard. He indicates that an outsource development firm was used to program portions of CaseGuard but this does not change the fact that source control was in fact used.

b. The fact that Defendants' programming partner utilized a source code control system while working on key portions of CaseGuard is further support of how unusual Defendants' claim is that they did not use source code control.

c. Defendant Abbas makes no effort to explain why replacing a computer in any way requires the destruction/disposal of the old computer. In fact, merely saving the old computer (as would be expected) is the simplest and most straightforward method for preserving the history and materials contained on the old computer.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 21st day of September, 2017, in Austin, Texas, Travis County.



Monty G. Myers

Exhibit 1

Microsoft Visual Studio using Version Control with the CaseGuard Application

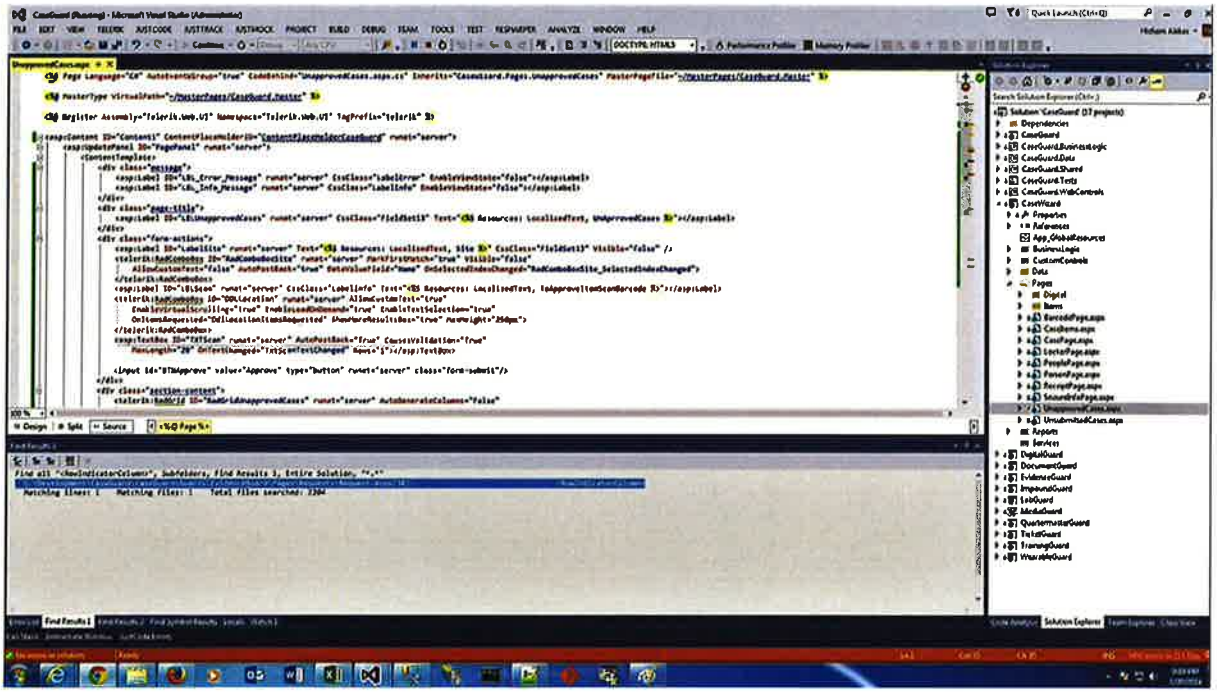


Exhibit 2

August 31, 2017 letter from Albert Wilson to Timothy McEvoy and Patrick McDonald

VEDA LAW
ATTORNEYS

www.vedalaw.com ▪ Tel: 240.839.4153 ▪ Fax: 202.315.3494

August 31, 2017

Via e-mail only to: Timothy McEvoy <TMcEvoy@cameronmcevoy.com>; Pat McDonald (PMcDonald@cameronmcevoy.com)

Timothy J. McEvoy, Esq.
Patrick J. McDonald, Esq.
Cameron/McEvoy PLLC
4100 Monument Corner Dr Ste 420
Fairfax, VA 22030

Re: Response to your e-mail dated August 25, 2017
QueTel v. Hisham Abbas, et al.
Case No. 17-cv-471-AJT

Dear Mr. McEvoy and Mr. McDonald:

Please accept this letter as our written response to your e-mail inquiry dated August 25, 2017. Your e-mail inquiry is set forth verbatim below.

> *Adam and Albert,*
>
> *Following entry of the Court's July 21, 2017 Order, Defendants produced images of the hard drives from a device that Defendants claim is the only device used in the development of CaseGuard. We have conducted a thorough forensic review of the images that were provided by Defendants at considerable expense to QueTel. It is clear that Defendants have, in fact, used a source code control system in developing CaseGuard. Per QueTel's Requests for Production of Documents to each Defendant, and the Court's Order of July 21, 2017, Defendants were required to produce and/or give us access to that source code control system, and produce all devices used for the development of CaseGuard. However, the source code control system has not been produced, nor have we been given access to it. Moreover, our review has revealed that the device imaged was only first used in September 2016, and, thus, could not have been the only device used for the development of CaseGuard We therefore insist that you remedy this issue immediately by providing us with access to the source code control system and turn over images of all devices used in CaseGuard's development. If Defendants contend that either the source code control system or any device used for CaseGuard's development is no longer in existence, please inform us immediately of when, how and why such was disposed of.*
>
> *Additionally, in response to Interrogatory No. 12 to finalcover, finalcover responded by identifying a laptop and "finalcover computers" as devices used in finalcover's business. Please identify the device for which the forensic images were produced, and state why forensic images of the other devices were not provided.*

Please advise on these matters no later than the close of business on Monday, August 28, 2017.

A. Devices Used Prior to 2016

As we discussed with you by telephone, Mr. Abbas purchased a new computer around September 2016. He disposed of his "old computer" in late 2016. Mr. Abbas represents that the old computer's contents were copied to the new computer.

B. Source Control System

In your e-mail, you wrote the following regarding a source control system: "*It is clear that Defendants have, in fact, used a source code control system in developing CaseGuard.*" Hisham Abbas represents the following: (1) while a source control system was installed on his "old computer," he did not use it to develop CaseGuard; (2) he copied his old computer's contents to a new computer but did not install a source control system on his new computer; (3) the forensic copy of his new computer did not contain a source control system because he did not install one; and (4) he does not have access to his old computer because it was disposed of in late 2016.

C. Additional Devices

In your e-mail, you wrote the following regarding additional devices:

Additionally, in response to Interrogatory No. 12 to finalcover, finalcover responded by identifying a laptop and "finalcover computers" as devices used in finalcover's business. Please identify the device for which the forensic images were produced, and state why forensic images of the other devices were not provided.

Your document request number 45 reads as follows:

A forensic image of each computer/server ***used for the production operation of the Target System including application****. database, and any other servers. If such computers/servers contain multiple storage devices, each storage device shall be imaged. The forensic image(s) shall be produced in a format compatible with EnCase.*[1]

Your document request number 46 reads as follows:

All documents and things relating to, referring to or evidencing the software developing environment in which the Target System was created, changed, improved or worked upon, including ***a forensic copy of the developing environment, the operating system and/or other software***

[1] Bold added.

> ***applications in which the Defendants created, changed, improved used and/or referred to any version of the Target System.***[2]

The forensic image that finalcover produced was taken from Hisham's computer. The "laptop" and other "finalcover computers" referenced in finalcover's responses to Interrogatory Number 12 were neither "*used for the production operation of the Target System including application,*" nor used for "*the developing environment, the operating system and/or other software applications in which the Defendants created, changed, improved used and/or referred to any version of the Target System.*" As such, no forensic image of those devices was produced.

Please contact me or Adam if you have any questions.

Sincerely,

/s/

Albert Wilson

cc: finalcover

---

[2] *Id.*

Exhibit 3

Cease and Desist Letter

Cameron / McEvoy PLLC

Matthew H. Sorensen
Attorney at Law
(703) 460-9342 (Direct)
msorensen@cameronmcevoy.com

May 16, 2016

URGENT – IMMEDIATE RESPONSE REQUIRED

Via Hand-delivery

Hisham Abbas and Shorouk Mansour
156 Magnolia Rd.
Sterling, VA 20164,

and

finalcover, LLC,
2115 Whitfield Place
Suite 201
Sterling, VA 20165

Re: *Cease and Desist Demand; Your Misappropriation and Infringement of QueTel Corporation's Trade Secret and Copyright Protected TraQ Suite 6 Software*

Dear Mr. Abbas and Ms. Mansour:

This firm represents Mr. Abbas' former employer, QueTel Corporation (hereinafter the "Company"). We are writing to demand that you immediately cease your ongoing unlawful misappropriation and infringement of the Company's trade secret and copyright-protected "TraQ Suite 6" software, including its software modules and its related source code (collectively, "TraQ Suite 6").

Specifically, and as set forth more fully below, the Company has recently been alerted that Mr. Abbas unlawfully and maliciously copied the code for TraQ Suite 6 during his employment with the Company, and that both of you (along with finalcover, LLC) are now using it as the basis for a competing offering called "CaseGuard." Accordingly, the Company is demanding that you provide the undersigned with an unequivocal commitment, in writing, that you will cease and desist from any and all further infringing uses of the Company's intellectual property, including, but not limited to, the computer software source code underlying TraQ Suite

4100 Monument Corner Drive, Suite 420 • Fairfax, Virginia 22030 TEL 703.273.8898 FAX 703.273.8897

6, no later than close of business on May 17, 2016, and as set forth below at the foot of this letter.

The Company is a pioneer in the field of asset tracking and evidence management systems for law enforcement agencies, and its leading product offerings are embodied in TraQ Suite 6. The components of TraQ Suite 6 include, but are not limited to, the following: (a) Evidence TraQ – a paperless physical evidence management software module; (b) Digital TraQ – a comprehensive digital evidence management software module, including video redaction; (c) Lab TraQ – a laboratory management software module; (d) Document TraQ – an optional software feature of Digital TraQ that provides a fully searchable document repository for voluminous digitized paper records; (e) Mobile TraQ – an app for iOS and Android devices that permits users to record images, videos, interviews and evidence, enter notes and evidence descriptions, scan witness and suspects' drivers' licenses, and upload that information to a central database that can be accessed by the other modules; (f) Cam TraQ – a high-speed, front-end upload software utility for body cameras; (g) Training TraQ – a training scheduling, tracking and management software module; (h) Quartermaster TraQ – an inventory management software module for equipment, uniforms and supplies (i) Impound TraQ – software designed to manage impounded and seized vehicles; and (k) Asset TraQ – software that tracks assets and manages inventories. These software solutions are referred to as "Modules" and may be licensed singly or in various configurations (up to, and including, all of the Modules in a comprehensive package). To function properly, each Module is connected to one core source code (the "Core Engine") that coordinates and powers the system's overall functionality, harmonizing the working of the Modules and promoting a seamless end-user experience. A user of any of the Company's Modules never "sees" or interacts directly with the core software code, and is not required to appreciate the distinction between the Modules and the Core Engine. Rather, a user experiences the software through an intuitive graphical user interface (known in the trade as "GUI") that can be accessed via computer or "smart device."

As you are well aware, the Company developed the Core Engine over a period of several months in 2009 and 2010, and since that time it has been the subject of substantial refinements. Development of those add-on refinements entailed months of work by the Company's development team. In total, the Company estimates that the development and refinement of TraQ Suite 6 (including, but not limited to, the Core Engine) has involved thousands of man hours and millions of dollars in total expense by the Company as of the date of this Cease and Desist Letter. Any competitor of the Company seeking to develop its own software code similar to that of TraQ Suite 6 through legitimate means would need to expend similarly significant resources in order to achieve such an end.

The source code for TraQ Suite 6 is an original work (for hire) that is subject to protection under United States copyright laws. On or about June 28, 2010, the Company sold the first application based on TraQ Suite 6 to a law enforcement agency in the United States. Accordingly, June 28, 2010 is the "publication" date of TraQ Suite 6. The Company registered its copyright in the TraQ Suite 6 software code on or about March 21, 2016 with the United States Copyright Office. Copies of the Certificate of Registration and the U.S. Copyright Office's online records reflecting this registration are attached hereto as Exhibit A. Accordingly, the code for the TraQ Suite 6 software is protected by the Copyright Act of 1976, 17 U.S.C. §

101 *et seq.* It is also protected by other laws, such as the Virginia Uniform Trade Secrets Act, Va. Code §59.1-336 *et seq.* (the "VUTSA").

Mr. Abbas was employed by the Company as a software developer from June 2007 through April 2014. During that time, the Company sponsored him for permanent resident status in the United States because he was a Syrian immigrant living in the United States on a student visa (at the time) and the Company valued him as an employee. In June of 2013, he assumed the role of lead software developer, which was the position he held through his last day of employment in April of 2014. Unfortunately, it has now become clear that Mr. Abbas used his position of trust and authority at the Company to steal the TraQ Suite 6 software (including, the Core Engine and the various software Modules) and its associated source code in order to carry out and promote a deliberate plan to infringe the Company's copyright- and trade secret-protected intellectual property.

In April of 2014, Mr. Abbas abruptly resigned from his employment with the Company. On May 28, 2014 finalcover, purchased the domain name "CaseGuard.com" from one Jason Newby and registered it under the names of Ms. Mansour, so as to conceal Mr. Abbas' involvement with CaseGuard from the Company. The registration of the "CaseGuard.com" domain was an essential element of an unlawful plan to infringe, and misappropriate, the Company's copyrighted code for the TraQ Suite 6 software. Like TraQ Suite 6, CaseGuard is a web-based asset tracking and evidence management software system. Accordingly, you needed to create a website (and thus register a domain for that website) in order to operate the infringing CaseGuard software and deliver it to customers and potential customers.

Within seven to eight months of Mr. Abbas' resignation from the Company, "Caseguard.com" was being used to market and promote the "CaseGuard" software, which consisted of a set of applications that had substantially the same functionality as the TraQ Suite 6 software. Moreover, we have obtained evidence that only a few months after Abbas' resignation from QueTel, the CaseGuard software was "up and running" with over 2,204 separate files of code. Further, the data entry screens for CaseGuard are almost exactly the same as those for the TraQ Suite 6 software. This was troubling, because the creation of CaseGuard and its various applications from scratch (without reference to the TraQ Suite 6 software) would have been a monumental undertaking, and it seemed highly unlikely that this could have been accomplished in the relevant time period without infringing upon the protected TraQ Suite 6 software source code.

The situation was very recently clarified, however, as the result of a number of coincidental events. Mr. Abbas sent a digital image of a page of the source code for CaseGuard to a friend who was (and remains) a Company employee. Mr. Abbas and his friend appear to have been communicating via social media about what color tie to wear to Mr. Abbas' wedding to Ms. Mansour. Mr. Abbas sent his friend an image of the tie on one of two side-by-side computer monitors that he was using as a workstation, which also displayed one of the pages of the CaseGuard code. A true and accurate copy of the page of the CaseGuard code that Mr. Abbas transmitted via social media post is attached hereto as Exhibit B. The source code shown in Exhibit B is identical for all relevant purposes to a portion of the code for the physical evidence Module of the TraQ Suite 6 software. That source code is not "off the shelf" code that

would be commonly used in any applications similar to the TraQ Suite 6 software, negating any inference of accidental or innocent similarities. Furthermore, the subject code is contained deep within the structure of the physical evidence Module, making it not only more likely than not, but almost certain, that the source code preceding and following what is contained in Exhibit B is identical or nearly identical to the corresponding code in TraQ Suite 6. If the CaseGuard physical evidence module is identical or nearly identical to the Company's physical evidence Module, and it surely appears to be, then it is not only more likely than not, but almost certain, that the Core Engine source code that CaseGuard uses is also identical or nearly identical to the Company's Core Engine. Accordingly, it is an irresistible conclusion that you have unlawfully replicated the overall structure, sequence and organization of the copyrighted and trade secret-protected TraQ Suite 6 software.

The Company has learned that this infringing conduct is now causing it actual economic harm. Very recently, you successfully solicited business from a long-time customer of the Company, the Maricopa County, Arizona Sheriff's Office. That customer has replaced one of the TraQ Suite 6 applications with a corresponding CaseGuard application. Making such a replacement was no doubt facilitated by the infringing similarity of CaseGuard to the TraQ Suite. Furthermore, you continue to offer the infringing CaseGuard software through your website. Even if this were not true, however, the Company is entitled to recover, among other things, statutory damages and its attorney's fees under the Copyright Act.

Your above-described actions constitute blatant violations of the federal Copyright Act and the VUTSA (as well as other statutes and relevant common law duties). Those unlawful actions have caused substantial harm to the Company's business and will continue to do so. In view of the foregoing, we hereby demand that you immediately:

(1) Cease and desist any and all further infringing uses of the Company's intellectual property, including but not limited to the computer software source code underlying the TraQ Suite 6 software;
(2) Cease and desist all advertising, promotion and sale of the CaseGuard software;
(3) Provide an accounting of all sales of the CaseGuard software made to date; and
(4) Allow the Company to copy and inspect a complete copy of all versions of the CaseGuard source code as well as any computers that Abbas has used during the period from January 1, 2014 to present.

Please acknowledge your compliance with these demands, or acceptance thereof, no later than the close of business on May 17, 2016.

Beyond the above-referenced obligations, **please be aware that you must preserve all potentially relevant evidence relating to the matters addressed in this letter.** This duty to preserve potentially relevant evidence extends to all such evidence, regardless of the format in which it may exist. It specifically includes, but is not limited to, any e-mails (whether in a personal or business e-mail account), any documents stored on any personal or business computers, servers, electronic storage devices, external hard-drives or other similar devices, and/or cloud storage accounts concerning the subject matter of this letter, CaseGuard and/or TraQ Suite 6. Failure to preserve such evidence may result in sanctions. The possible

sanctions include an inference in judicial proceedings that the failure to preserve such evidence indicates knowledge of wrongdoing and liability, and that any destroyed evidence would have helped establish the Company's claims, as well as monetary and other judicially imposed sanctions.

The Company takes this matter very seriously and is prepared to take action to enforce its legal rights.

We look forward to your very prompt response.

Very truly yours,

Matthew H. Sorensen

cc: Client
Timothy J. McEvoy, Esq.

Certificate of Registration

This Certificate issued under the seal of the Copyright Office in accordance with title 17, *United States Code*, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

Maria A. Pallante

United States Register of Copyrights and Director

Registration Number
TX 8-167-420
Effective Date of Registration:
March 21, 2016

Title

Title of Work: Traq Suite 6

Completion/Publication

Year of Completion: 2010
Date of 1st Publication: June 28, 2010
Nation of 1st Publication: United States

Author

Author: Quetel Corporation
Author Created: computer program
Work made for hire: Yes
Domiciled in: United States

Copyright Claimant

Copyright Claimant: Quetel Corporation
14100 Sullyfield Circle, Suite 700, Chantilly, VA, 20151, United States

Rights and Permissions

Organization Name: Quetel Corporation
Name: James Cleaveland
Email: jrc@quetel.com
Telephone: (703)318-6834
Alt. Telephone: (703)819-4430
Address: 14100 Sullyfield Circle
Suite 700
Chantilly, VA 20151 United States

Certification

Name: James R. Cleaveland
Date: March 21, 2016

Type of Work: Computer File

Registration Number / Date:
TX0008167420 / 2016-03-21

Application Title: Traq Suite 6.

Title: Traq Suite 6.

Description: Electronic file (eService)

Copyright Claimant:
Quetel Corporation.

Date of Creation: 2010

Date of Publication:
2010-06-28

Nation of First Publication:
United States

Authorship on Application:
Quetel Corporation, employer for hire; Domicile: United States. Authorship: computer program.

Rights and Permissions:
James Cleaveland, Quetel Corporation, 14100 Sullyfield Circle, Suite 700, Chantilly, VA, 20151, United States, (703) 318-6834, (703) 819-4430, jrc@quetel.com

Names: Quetel Corporation

==========

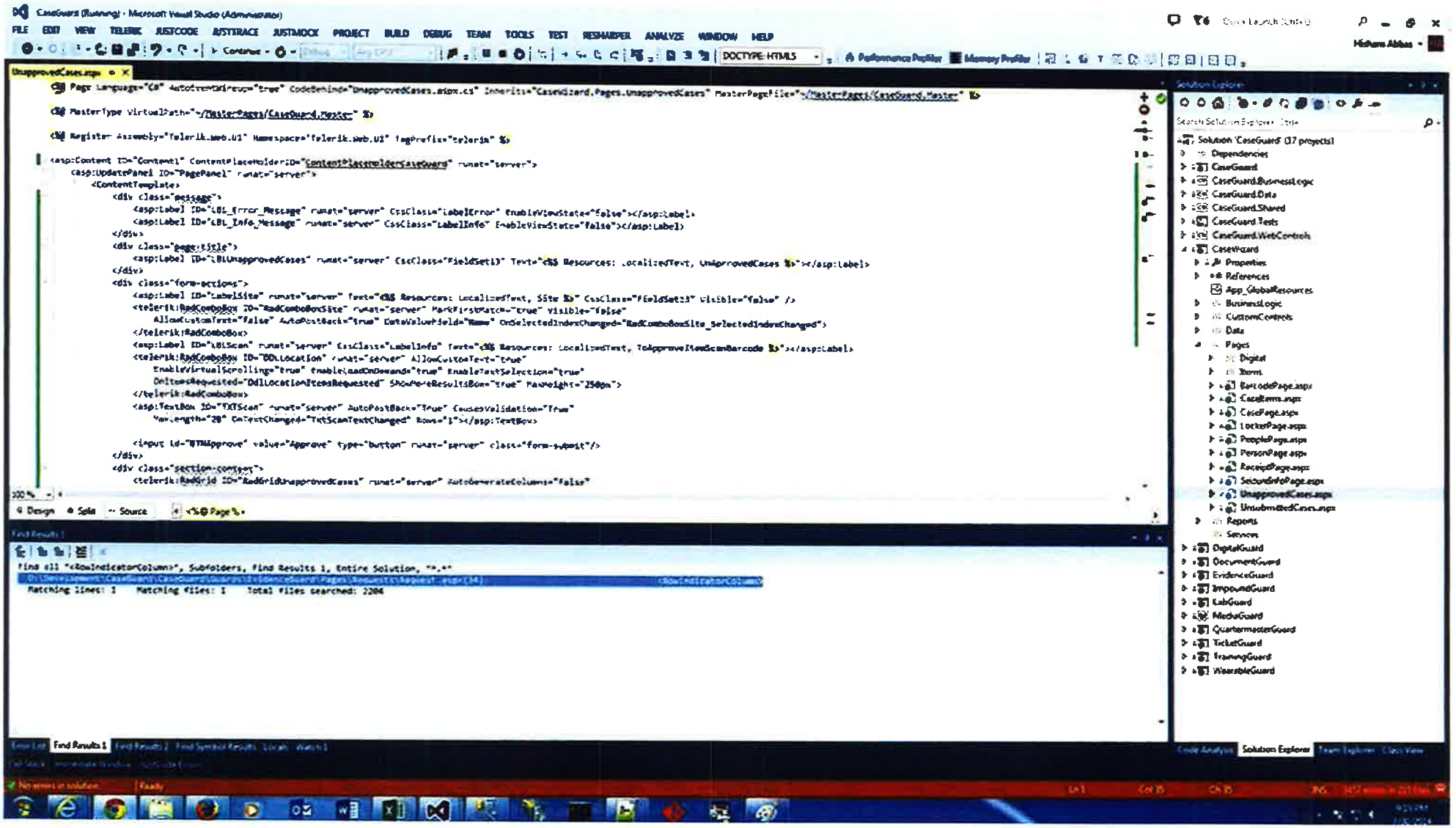


Exhibit 4

CaseGuard .svn folder

Exhibit 5

Uninstallation of Git Bash Client

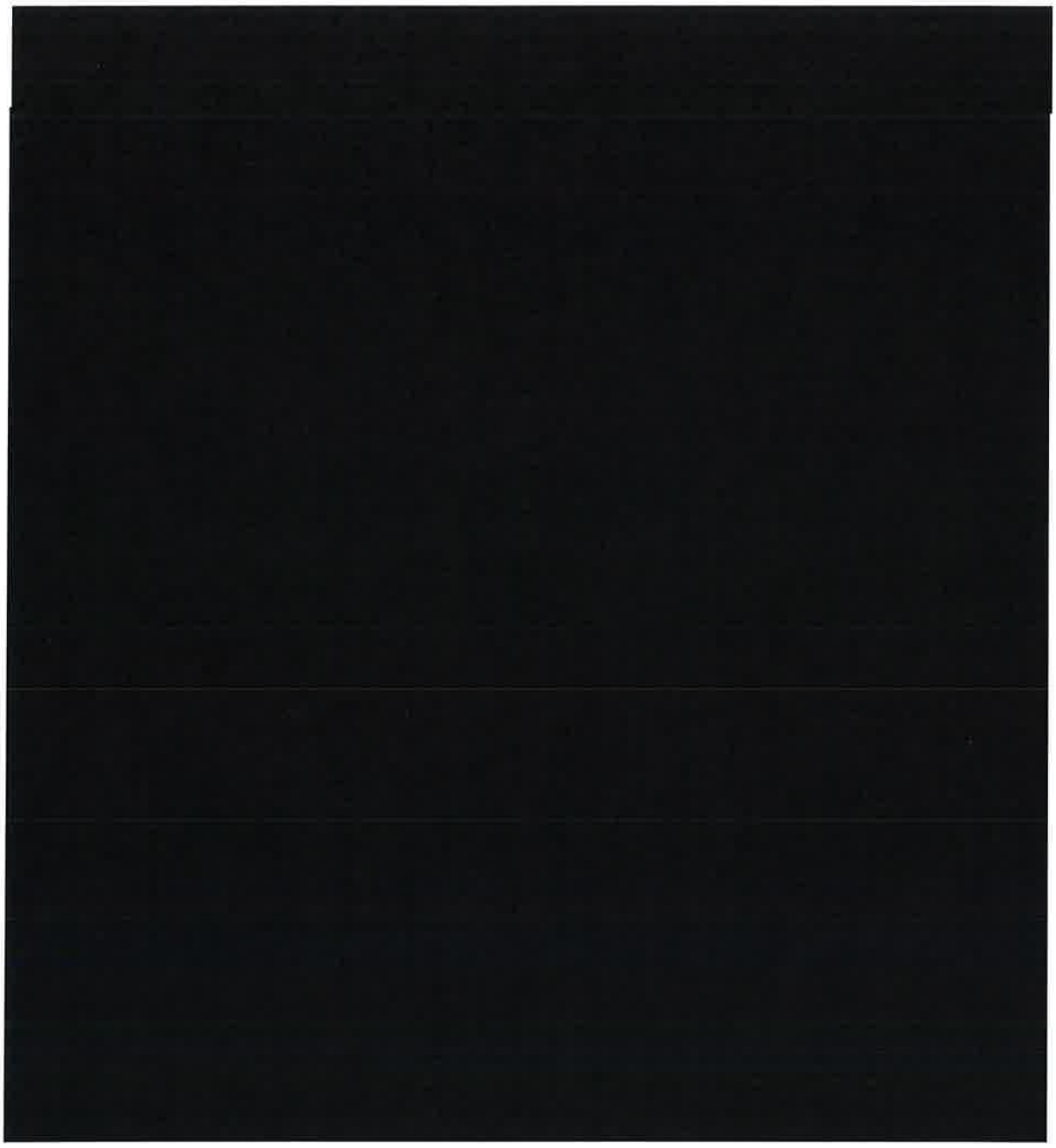


Exhibit 6

Defense Counsel's letter dated September 14, 2017

VEDA LAW
ATTORNEYS

www.vedalaw.com • Tel: 240.839.4153 • Fax: 202.315.3494

September 14, 2017

Via e-mail only to:
Timothy McEvoy (TMcEvoy@cameronmcevoy.com)
Pat McDonald (PMcDonald@cameronmcevoy.com)

Patrick J. McDonald, Esq.
Timothy McEvoy, Esq.
Cameron/McEvoy PLLC
4100 Monument Corner Dr, Ste 420
Fairfax, VA 22030

Re: finalcover's response to your letter dated September 8, 2017
Quetel Corp. v. Hisham Abbas, et al.
Case No.: 17-CV-471

Dear Messrs. McDonald and McEvoy:

In your letter dated September 8, 2017, you raised several issues. We respond to each below:

In your letter, you wrote:

> *You have now received QueTel Corporation's Expert Witness Disclosure, which includes the report from Monty G. Myers. In his report, Mr. Myers makes, among others, the following findings:*
>
> *(1) "The [screenshot] shows the use of a source code control system at that time for CaseGuard development.*
>
> *(2) "Forensic analysis of Defendant Abbas' computer images shows evidence of the use of both Subversion and Git source code control systems within the CaseGuard project.*

(3) There is "[e]vidence that Defendant uninstalled Git just 6 days before the forensic images were made.

1. QueTel asserts: "The [screenshot] shows the use of a source code control system at that time for CaseGuard development."

In terms of the timeline, the "screenshot" to which you refer was taken in 2014. Based on QueTel's answers to finalcover's request for admissions, you were aware of the screenshot in 2014. About two years later, QueTel's attorney, Matthew Sorensen, sent a cease-and-desist letter to finalcover. In the letter, QueTel accused finalcover of stealing QueTel's code (TraQ Suite 6). Upon receipt of your letter, finalcover through its counsel responded. Further, finalcover waited before replacing its computer to see whether QueTel would file a legal action. After perhaps five months or so, finalcover decided to replace the six-year-old computer that it had used to develop CaseGuard. Almost one year after QueTel sent its cease-and-desist letter, QueTel sued finalcover in April 2017.

As you now know, finalcover replaced the computer that it used in 2014 to develop CaseGuard. We submit that finalcover's decision to replace the computer was not done with a culpable state of mind. *See Sampson v. City of Cambridge*, 251 F.R.D. 172, 181 (D. Md. 2008) (discussing burden to satisfy elements of spoliation including demonstrating culpable mind). Indeed, finalcover waited months to see if QueTel would take legal action before replacing its six-year-old computer.

2. QueTel asserts: "Forensic analysis of Defendant Abbas' computer images shows evidence of the use of both Subversion and Git source code control systems within the CaseGuard project."

We cannot agree with your expert's assessment. In brief, the mere presence of either "Subversion" or "Git" files do not establish a source control system was used in the development of the Case Guard Software. The source of the "Subversion" or "Git" files could have, and we submit, did come from other sources.

Most of the Git files come from the Android folder contained within the CaseGuard software. This software was written by a company located in India. They employed Git for their source control repository and used Subversion as their source control mechanism while building the iOS and Android mobile applications.

It is also important to note that any developer will have Git files on their machine, as all developers download lots of source code that come from Github.com. When you download this source code, you typically also receive Git files.

3. QueTel Asserts: "'There is '[e]vidence that Defendant uninstalled Git just 6 days before the forensic images were made.'"

The alleged uninstallation of the Git software would not necessarily remove any of the code that was being tracked by Git. If there was a Git repository on the machine there would have been traces of that repository in the registry or in other locations that your forensics report would have noted. As you know, a claim of spoliation of evidence involves a determination of what prejudice the moving party has suffered. *Sampson,* 251 F.R.D. at 180 (discussing the moving party's burden to establish prejudice). Here, given that the alleged uninstallation would not have necessarily removed any code, we cannot, at this time, identify what if any prejudice QueTel has suffered. What's more, finalcover has produced a full and complete copy of its code, which is the critical issue in this case.

Defendant's Discovery Responses

You assert that Defendants' responses to QueTel's discovery requests are deficient and in need of prompt supplementation. Our response is below.

A. Defendants' objection to Plaintiff's First Set of Requests

1. Missing e-mail attachments

If we produced e-mails without the attachments, we will provide them without delay. We will need to review the e-mails produced and whether these e-mails contained attachments that were not produced. We'd ask that you give us until **Tuesday, September 19, 2017** to produce any missing attachments.

2. Documents concerning actual sales, projected unit sales, revenue, gross profits and/or losses, operating profits or losses, and costs associated with the Target System

As you know, Rule 34 does not impose a duty to create documents. *See Harris v. Advance Am. Cash Advance Ctrs.*, 288 F.R.D. 170, 172 (S.D. Ohio 2012) (defendants not required to create documents). finalcover has not created the requested documents. As such, few if any were produced. We will, however, seek to confirm whether finalcover possesses such documents. We'd ask that you give us until **Tuesday, September 19, 2017** to produce any additional responsive documents.

3. Spousal Privilege

We will verify whether any documents were withheld based on spousal privilege. But during our initial production, we do not believe that documents were withheld based on spousal privilege. We'd ask that you give us until **Tuesday, September 19, 2017** to produce any additional responsive documents.

B. Defendants' Responses to Plaintiff's First Set of Interrogatories

Your Comments:

finalcover and Abbas' Answer to Interrogatory No. 1:
Interrogatory No. 1 to finalcover and Abbas asks those Defendants to identify all persons and/or entities involved in the development, revision, maintenance and/or improvement of the Target System (including but not limited to, any and all independent contractors, subcontractors or other persons or entities who contributed in any way to the development, revision, maintenance and/or improvement of the Target System and/or from whom You and/or any of the other Defendants licensed or otherwise obtained any software, systems, equipment and/or other materials used in connection with the development, revision, maintenance and/or improvement of the Target System). finalcover and Abbas have identified twelve individuals/entities, but have failed to provide contact information for nine of them. "Identify", with respect to persons, is defined in the Interrogatories to require such contact information. Please supplement by providing all last known contact information for every individual/entity identified.

Response: We will supplement our response to this interrogatory. responsive documents.

finalcover and Abbas' Response to Interrogatory No. 2:
These Interrogatories call for finalcover and Abbas to describe in detail the nature and substance of the involvement of any person and/or entity identified in response to Interrogatory No. 1 in the development, revision, maintenance and/or improvement of the Target System, including, but not limited to, the dates of such person or entity's involvement and the nature and substance of any goods and/or services that such person or entity provided in connection with the development, revision and/or improvement of the Target System. finalcover and Abbas have failed to provide the requisite level of detail regarding the nature and substance of each identified person's or entity's involvement. Please supplement to provide all responsive information.

Response: We will supplement our response to this interrogatory.

Finalcover and Abbas' Response to Interrogatory No. 4:
These Interrogatories call for finalcover and Abbas to identify all versions of CaseGuard and to describe in detail the differences from one version to the next. finalcover and Abbas have failed in their responses to describe

the differences between the versions identified in any detail, let alone with sufficient detail. Please supplement accordingly

Response: We will supplement our response to this interrogatory.

finalcover and Abbas' Response to Interrogatory No. 6: *These Interrogatories ask finalcover and Abbas to describe in detail the process by which CaseGuard was developed. finalcover and Abbas have provided only a cursory description. Please supplement to include a full and complete response.*

Response: We will supplement our response to this interrogatory.

finalcover and Abbas' Response to Interrogatory No. 8: *These Interrogatories ask finalcover and Abbas to identify any and all materials one or more Defendants consulted and/or reviewed in connection with the creation and/or revision of the source code for CaseGuard, and describe in detail the manner in which each such material was used in connection with the creation and/or revision of CaseGuard's source code. finalcover and Abbas have failed in their answers to describe in detail the manner in which the identified material was used. Please supplement accordingly.*

Response: We will supplement our response to this interrogatory.

finalcover and Abbas' Response to Interrogatory No. 11, Mansour's Response to Interrogatory No. 3: *These Interrogatories ask Defendants to identify and describe in detail any and all communications between each Defendant and any other person or entity concerning Abbas Employment Agreement. Defendants have not answered, and, instead, have objected on the following grounds: finalcover and Abbas timely objected on the grounds of attorney/client privilege, and, in an untimely manner, objected on the grounds that the Abbas Employment Agreement has not been produced. Mansour timely objected to this Interrogatory on the ground that the Interrogatory is overly broad, and not reasonably calculated to lead to the discovery of admissible evidence, and, in an untimely manner, objected on the grounds of the spousal and attorney/client privileges. Notably, Abbas did not claim spousal privilege, and, thus, has waived that privilege. Next, as to all untimely objections, they are waived. Second, the Court ordered Defendants to produce a privilege log at the hearing in this matter on July 21, 2017, for all privileges. As noted above, Defendants' privilege log fails to log any. spousal communications. As such, even if the spousal privilege was timely, it has since been waived by the failure to log such communications. The objections related to overbreadth and*

Response: We will verify whether any documents were withheld based on spousal privilege. But during our initial production, we do not believe that documents were withheld based on spousal privilege. As you know, in lieu of setting forth all communications, we may simply produce documents reflecting those communications.

> ***finalcover and Abbas' Responses to Interrogatory No. 15:*** *These Interrogatories ask finalcover and Abbas to describe in detail the full factual basis for their defense that the source code for TraQ Suite and/or TraQ Suite 6 is actually open source code, identifying with particularity any and all portions of the source code that they claim are open source. finalcover and Abbas have provided only general responses, failing to identify with particularity those specific portions of TraQ Suite/TraQ Suite 6's code that they claim as open source. Please supplement accordingly.*

Response: We will supplement our response to this interrogatory.

> ***Mansour's Responses to Interrogatory Nos. 2 & 6:*** *These Interrogatories call for Mansour to identify and describe in detail any and all communications (a) between her and any other person or entity concerning TraQ Suite and/or TraQ Suite 6 from the date on which Abbas resigned from his former employment with QueTel through the present (Interrogatory No. 2), and (b) between her and Abbas concerning Abbas' intent to resign from his former employment with QueTel and/or his actual resignation from QueTel. Mansour's objections, save for spousal privilege, were overruled at the hearing on July 21, 2017. Moreover, Mansour has failed to log any communications between her an Abbas that would be responsive to this Interrogatory, as she was ordered to do. As such, the spousal privilege has now been waived. Please provide a full and complete response to these Interrogatories, without objection.*

Response: None.

Defendants' Request for Additional Time

We'd ask that you give us until **Tuesday, September 19, 2017** to produce any additional responsive documents and to provide supplemental responses to interrogatories.

If you have any questions or concerns, please feel free to call me at (240) 839-4153.

Very truly yours,

/s/

Albert Wilson, Jr.
David Adam Devries

cc: finalcover, LLC